AGING, COUNTERFEITING CONFIGURATION CONTROL (AC3)

FINAL REPORT

Sergio R. Gallardo
Performance Management
Supply Chain Management
Raytheon Missile Systems

Mark Kelly
Director of Services
Renaissance Services

Dr. William "Chuck" Louisell
TDSC Technical Director
Alion Science & Technology

Goran Bencun
Program Manager
Advanced Core Concepts

Dennis Simon
TDSC Senior Program Manager
Advanced Technology International

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
31-01-2010	Final Technical Report AC3	NOV 2009-DEC 2010

4. TITLE AND SUBTITLE

Aging Counterfeit Configuration Control Project Final Technical Report

5a. CONTRACT NUMBER

HQ0006-05-C-003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dennis Simon Advanced Technology International (ATI)
Sergio Gallardo Raytheon Missile Systems
Goran Bencun Advanced Core Concepts
Dr. William C. Louisell Alion Science and Technology

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

ATI
5300 International Blvd
North Charleston, South Carolina 29418

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Manufacturing and Producibility (MP)
Missile Defense Agency
5611 Columbia Pike
Arlington, VA 22202

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Counterfeit parts including recycled and relabeled microcircuit chips threaten the reliability, safety, and performance of DoD systems. DoD systems are particularly susceptible to intrusion of counterfeit parts, because of increasing reliance on commercial off the shelf (COTS) electronic components and microprocessors. AC3 was deployed in a proof-of-concept format using real world data and electronics intensive guidance sub-assemblies within Standard Missile 3 (SM-3) which is the seaborne theater ballistic missile defense system of the US Navy. AC3 was designed to put into practice anti-counterfeiting strategies including three major thrusts: addressing reduction in the risk of acquiring counterfeit parts; reduction in the time to identify the impact of counterfeit alert notices; and reduction in the time required to identify the specific location of suspect parts. AC3 was designed to provide much-needed VISIBILITY into the supply chain at the COMPONENT level.

15. SUBJECT TERMS

Anti-Counterfeiting, GIDEP, component visibility, configuration control

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STEVE LINDER
UNCLAS	UNCLAS	UNCLAS	UU	28	19b. TELEPHONE NUMBER *(Include area code)* (703) 607-5319

Table of Contents

ACKNOWLEDGEMENT

The Transforming Defense Supply Chains (TDSC) Aging, Counterfeiting Configuration Control (AC^3) team wishes to recognize and thank Mr. Steve Linder from Missile Defense Agency Manufacturing and Producibility division for his steadfast support throughout this project and previous projects. Steve has been the consummate professional in the time we have worked for him. He has the unique ability to recognize disparate technologies and apply them to solve complex manufacturing and supply chain issues at hand. The team also wishes to thank the Joint Defense Manufacturing Technology Panel under the leadership of Dr. Brench Boden of the USAF Research Labs for funding this AC^3 project. Furthermore the team wishes to thank the support provided by Raytheon Missile Systems in the person of Frank Bernard who recognized the potential of the technology and potential cost avoidance. The team looks forward to deploying the completed tool at Raytheon in a true production environment, for as much as we like the challenge associated with development, the success of these Manufacturing Technology developments is in deployment of these systems.

EXECUTIVE SUMMARY

Counterfeit parts including recycled and relabeled microcircuit chips threaten the reliability, safety, and performance of DoD systems. DoD systems are particularly susceptible to intrusion of counterfeit parts, especially during surge and extended production runs, because of increasing reliance on commercial off the shelf (COTS) electronic components and microprocessors with short production lifecycles and the extended life of some systems past their planned dates of obsolescence. Restricting the supply chain to Original Component Manufacturers (OCM) and Factory Authorized Distributors (FAD) creates a supply chain "fortress" with positive control from manufacturing to installation seems like an effective strategy, it is not practical because of DoD system reliance on legacy components for aging weapons systems and internal processes at the "fortress" sites and due to cost. There have even been documented cases where counterfeit parts have infiltrated the "fortress" system through customer returns which included counterfeit parts which were not detected through the receipt process. The Aging, Counterfeiting Configuration Control (AC^3) project was funded by the Joint Defense Manufacturing Technology Panel Industrial Base Innovation Fund to identify cost effective methods to reduce counterfeit risk. The project was executed by the Missile Defense Agency (MDA) via the Transforming Defense Supply Chains (TDSC) program in partnership with Raytheon Missile Systems (RMS). The software application was designed to put into practice anti-counterfeiting strategies being explored by the aerospace and defense community including three major thrusts: addressing reduction in the risk of acquiring counterfeit parts; reduction in the time to identify the impact of counterfeit alert notices; and reduction in the time required to identify the specific location of suspect parts. AC^3 was designed to provide much-needed *visibility* into the supply chain at the *component level*.

AC^3 was deployed in a proof-of-concept format using real world data and electronics intensive guidance sub-assemblies within Standard Missile 3 (SM-3) which is the seaborne (and soon to be landborne) theater ballistic missile defense system of the US Navy and Japanese Maritime Self Defense Force. The proof-of concept application was evaluated using key metrics identified by the joint TDSC – RMS project team including: the number of man-hours consumed to support an alert driven investigative action, the degree of human dependency for data review and integration, the number of investigative path decisions requiring human interpretation of digital data, and the time that the production process would continue in an "at-risk" state while the investigation was conducted.

The Government Industry Date Exchange Program (GIDEP) is the current method for distributing data on discovered obsolete and counterfeit mechanical, electro-mechanical and electrical components. GIDEP has been criticized for slow or incomplete reporting. Companies were reluctant to report incidents due to liability concerns. GIDEP alerts were not fully distributed throughout the DoD prior to the affected supplier reviewing and appealing the instance of providing counterfeit or obsolete parts. While the review and appeal process were underway, more time and opportunities are available for the counterfeit or obsolete part to be installed. Recent policy changes to not wait to identify the specific supplier who provided the part, will reduce the time available to install potentially counterfeit parts, and the removal of liability concerns means that the number of GIDEP alerts is expected to increase from 4 to 5 per month to ***40 or 50***. It is recognized by all concerned that a tenfold increase in the number of GIDEP alerts processed on a monthly basis will overwhelm the existing capabilities of the prime contractors to review and adjudicate reports.

Implementation of AC^3 reduces the complexity and time of the RMS Government Industry Data Exchange Program (GIDEP) Alert processing procedure by automating 19 independent data searches performed by 5 organizations supporting 6 human-in-the-loop decision points. Automation reduced the potential for human error, the level of effort, the dependency on human data interpretation, and the elapsed investigation time. The results are summarized below.

Table 1: Man-Hours saved with AC^3

	Man-hours	Human Information Integration Dependency	Human Investigative Path Decisions	Investigative Time
W/O AC^3	4 hours	Very High	6	48 hours
W/ AC^3	< 30 minutes	Very Low	1	< 30 minutes

It is clear that an automated AC^3 GIDEP significantly reduces the time and labor to search and intercede.

RMS determined that the AC3 proof of concept was successful. Steps are in progress utilizing internal RMS Six-Sigma teams to **deploy** AC^3 in a production environment at RMS. AC^3 provided value, even with a minimum number of parts currently tracked by lot number or date code. The following table, provided by Raytheon Missile Systems summarizes the annual cost avoidance associated with a deployed AC^3 system at RMS, provided that all the systems were fully integrated. There would still be manual intervention required for weapons systems that were not fully integrated. The table below presents a best case scenario for cost avoidance using AC3 on all RMS weapons systems.

Table 2: Cost Avoidance with AC^3

GIDEP ALERTS	Weekly Alerts	Yearly Alerts (52 wks)	Effort (hrs) (4/GIDEP)	Cost ($135/hr)
Low	40	2080	8320	$ 1,123,200
High	50	2600	10400	$ 1,404,000

More importantly, the operational readiness of the missile systems will improve and the chance of a successfully accomplishment of the mission will increase.

1 INTRODUCTION

What happens when a counterfeit or obsolete part enters your inventory? Too often the reporting process is too slow, alarms are not activated and the suspect parts are installed and delivered. Without end-to-end visibility tracing the part and material pathways from purchase to installation and end-item delivery, it is difficult if not impossible, to determine the degree and distribution of risk associated with counterfeit parts.

While no one knows the actual extent of counterfeit parts that make their way into DoD weapons systems experts have postulated a range that is alarming. On the high end of the range, Mr. Robert Ernst from the NAVAIR Joint Committee on Aging Aircraft (JCAA) was quoted in a Fall 2008 *Newsweek* article stating that up to *15% of all flight parts in the DOD inventory may be counterfeit*. On the low end of the range, Pentagon spokesmen have stated that the percentage is less than one-half percent (0.5%). Considering the potential consequences from a system failure, even 0.5% constitutes a significant risk. Counterfeit parts- especially recycled and relabeled fake microcircuit chips from overseas - threaten the reliability, safety, and performance of DoD systems. These systems are vulnerable, especially during production surges in mature weapons systems and their block upgrade derivatives, because of the reliance on legacy electronic components which have a high probability that the components are out of production and are obsolete.

Intercepting a nuclear tipped reentry body is an extremely complex task; it is far easier to send a manned mission to the lunar surface- the moon is a much bigger and slower target. Failure to intercept a warhead because of a malfunctioning counterfeit part would be a cataclysmic event that could lead to the death of millions and probable war. The mission of MDA would be compromised by the failure of an SM-3 missile and exoatmospheric kill vehicle to intercept an incoming North Korean Taipo Dong II reentry body warhead due to a counterfeit part failure. The mission failure would be cataclysmic in terms of human lives, property and civilized world order. The reentry body intercept problem requires many disparate systems working perfectly and seamlessly to sense, track, and destroy a weapon moving a many miles per second outside the earth's atmosphere. Specialized electronic components are needed to withstand the harsh environment and operating conditions of exoatmospheric flight including high acceleration, temperature extremes, and radiation hazards. It is difficult to determine which components are certified to operate in these environments if they look the same as genuine parts and have the correct markings

As awareness of counterfeit parts grows, counterfeiters are becoming more sophisticated in the packaging and labeling of recycled parts and materials. Acetone swipes were all that was once needed to distinguish a counterfeit part due to the substandard marking. It is now more difficult for prime contractors and sub-tier suppliers to distinguish counterfeit parts from legitimate parts due to increasing sophistication on the part of the counterfeiters. One response may be to restrict the supply chain sources, requiring that prime contractors and sub-tier suppliers use only parts purchased from the Original Component Manufacturers (OCM) through Factory Authorized Distributors (FAD) creating a "fortress" with positive control of the article from manufacturing to installation. While this "fortress" approach may reduce the risk of counterfeit incursion into the supply chain, it is not necessarily practical because of the heavy reliance of DoD systems on components that are no longer in production and the additional cost of the "fortress" strategy. This issue is caused by the mismatch in component production cycle and weapons system acquisition cycle lengths, and drives the industrial

base to sources of supply other than the OCMs. Industry must look to secondary sources (Brokers) who can locate reserve parts that may exist in excess inventories held by a wide range of industrial base sectors. In a weapons system surge or extended production run scenario, parts from outside trusted supplier paths may be required to meet schedule demand. Additionally return procedures at Factory Authorized Distributors have resulted in the introduction of counterfeit parts into the inventory of OCMs and FAD "inside the fortress". The fact is - counterfeit parts can and do make it into the "fortress" inventory.

To address the detrimental impact of counterfeit parts on mission assurance, the Joint Defense Manufacturing Technology Panel (JDMTP) Industrial Base Innovation Fund (IBIF) sponsored a proof of concept (POC) project under the direction of Mr. Steve Linder at the Missile Defense Agency (MDA) Directorate for Producibility. The project was executed by the Transforming Defense Supply Chains (TDSC) Program – an effort aimed at identifying technical solutions to supply chain related mission assurance concerns. The project was implemented at Raytheon Missile Systems (RMS) in Tucson, AZ with the objective to develop a system which provides part and material visibility and traceability from item purchase through system delivery by tail number. The project called for development of a software application entitled Aging, Counterfeiting Configuration Control system or AC^3. AC^3 is a Service Oriented Architecture (SOA) that integrates data resident in enterprise information systems to provide program managers, supply chain personnel, and quality control personnel a counterfeit risk reduction dashboard.

AC^3 operates as an SOA within the RMS enterprise information technology environment. AC^3 is deployed behind the RMS corporate firewall calling on data generated and housed in enterprise-wide and functional area specific databases via a standing report protocol and a virtual data warehouse. Minimal data requirements include supplier records, purchasing records, testing records, design data, and configuration management records. AC3 was designed to meet the configuration control and verification requirements of the MDA Parts Materials and Processes Mission Assurance Plan (PMAP) which was cited by report GAO-10-389 of March 2010 as being an initiative that should be leveraged throughout DoD. AC^3 is readily extensible into a full-scale deployment offering a cost effective means of implementing MDA and DoD required practices to reduce the potential for counterfeit incursion. Internal RMS 6-Sigma teams are beginning the preliminary work to deploy AC^3 at Raytheon Tucson.

2 PROOF-OF-CONCEPT DESCRIPTION

2.1 THE COUNTERFEIT RISK ASSESSMENT PROCESS

The AC^3 application was designed on an RMS review of existing counterfeit related management practices aimed at identifying vulnerability to counterfeit parts introduction. The goal of the review was to identify candidate practices and information requirements that would form the basis for software design use cases and data system architectures. As a precursor, interviews were conducted to identify the root causes that created opportunity for counterfeit parts and to map the range of possible incursion pathways.

The RMS reviews identified a range of root causes and multiple incursion pathways supporting the potential for counterfeiting. The driving cause was found to be obsolescence. Production cycles on electronic parts are generally short-runs driven by commercial market needs. Expiration of the production runs creates a future availability problem that drives vendors and consumers to make

purchase decisions based on anticipated defense acquisition levels. This creates an environment in which various entities experience surpluses and others experience shortages. The incursion pathways emerge in the years following the end of production as excess inventories are redistributed following a supply and demand flow model in which parts and materials may be purchased by one or more intermediate brokers for immediate resale or, in some cases, for stockpiling to meet anticipated future demand. At the same time, commercial products using the same components reach the end of their lifecycle and are disposed of. Some of the components are salvaged, reconditioned, and intentionally re-introduced into the market place as new products

Based on the reviews, three distinct elements were identified for inclusion in effective counterfeit risk reduction strategies and to provide visibility into installed system components. The first is reduction in the risk of acquiring counterfeit parts and introducing them into the production process. The second is rapid identification of the impact of counterfeit alert notices by providing visibility into which other systems are affected by tail number and other components provided by this supplier. The third is rapid identification of the location of suspect parts within the system of interest such that the suspect parts can be intercepted at the earliest point within the production cycle reducing the need to perform general recalls and inspections. These findings formed the high level functions to be performed by AC^3.

The first function provides a proactive view of the systemic risk associated with parts and materials that make up integrated systems. The function allows project managers, supply chain managers, and quality assurance managers to see how purchasing practices, acceptance practices, and inventory handling practices influence the potential for a counterfeit to make its way into a full-up delivered missile. This function allows program managers to see where the potential for counterfeits is highest. Risky sources of supply are identified, as well as, risky categories of suppliers. This is supported by a comparison with part and material criticality index supporting decisions relative to modifying practices on a cost – consequence basis.

The second function provides a reactive protocol driven response to counterfeit alert notifications providing specialists across the enterprise with a rapid impact assessment of the potential that an alert generated by external or internal sources affects parts and materials in the design on hand or in work. This function reduces the time required to identify impact, reduces the potential for human error in record searches, and reduces the time required to generate decision quality information to support risk mitigation actions.

The third function is visibility. This function brings production part and material specific data records into a rapid assessment environment that identifies specifically affected components, assemblies, sub-systems, and systems providing a "by tail number" location of any parts or materials affected by the counterfeit alert notice.

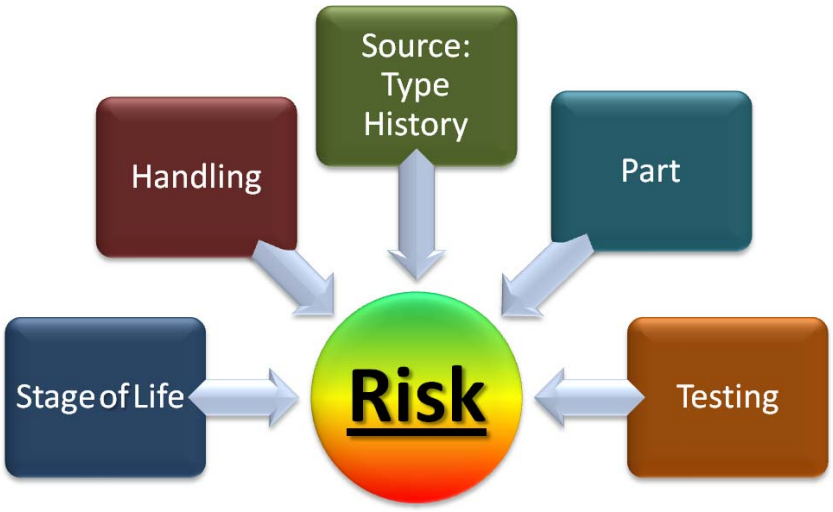
2.2 PROACTIVE RISK COUNTERFEIT ASSESSMENT

Proactive risk assessment is an important element of the strategy. It is aimed at reducing the probability of counterfeit parts making their way into the production environment. The approach employed within the AC^3 application is designed to allow prime contractors to see the risk topology that is generated by component and sub-system procurement practices. The algorithm – Supplier Assessment Risk Algorithm (SARA) – examines readily available supplier and component and sub-system

procurement related information as a means to establish a relative risk index for each component and/or sub-system. The relative index system allows the prime contractor to set threshold levels that will command management attention. Threshold levels can be set relative to consequence potential in terms of impact on system performance or can be set relative to a defined component or sub-system criticality class such as those defined within the Missile Defense Agency PMAP (Parts Material Assurance Plan). When limited sources of supply force procurement from a questionable source; scrutiny can be increased in the receipt process to reduce the risk of a counterfeit or obsolete part entering the inventory.

Proactive risk assessment is accomplished by examination of information relative to parts and materials. The information establishes a "pedigree" that is used within the AC^3 proactive risk algorithm – SARA. The basis for SARA was a set of influencing factors identified and defined by a joint TDSC – RMS team. The team's objective was to identify elements of the pedigree that were reasonably available given the information available in disparate enterprise databases. The condensed influence diagram summarizing this effort is shown below.

Figure 1: SARA Risk – High Level Architecture



SARA is based on the detailed influence diagram developed by the joint team. SARA translates the detailed influence diagram in to a computational structure to support assessment activities in three key areas of interest - the nature of the part or material, the nature of the source, and the nature of the testing the part or material undergoes prior to installation. Within these three key areas, seven key attributes were identified and each of the attributes was assigned various 'linguistic" values for entry into the algorithm. The three values represent a range from "counterfeit potential reducing" through "neutral" to "counterfeit potential increasing". The table below summarizes the SARA inputs.

Table 3: SARA Inputs

Nature of the Part or Material

- Stage of Component Lifecycle
  - Early Stage
  - Middle Stage
  - Late Stage
- Inventory Handling Practices
  - Serial Number Tracked Object
  - Lot Number Tracked Object
  - Untracked Object

Nature of the Source

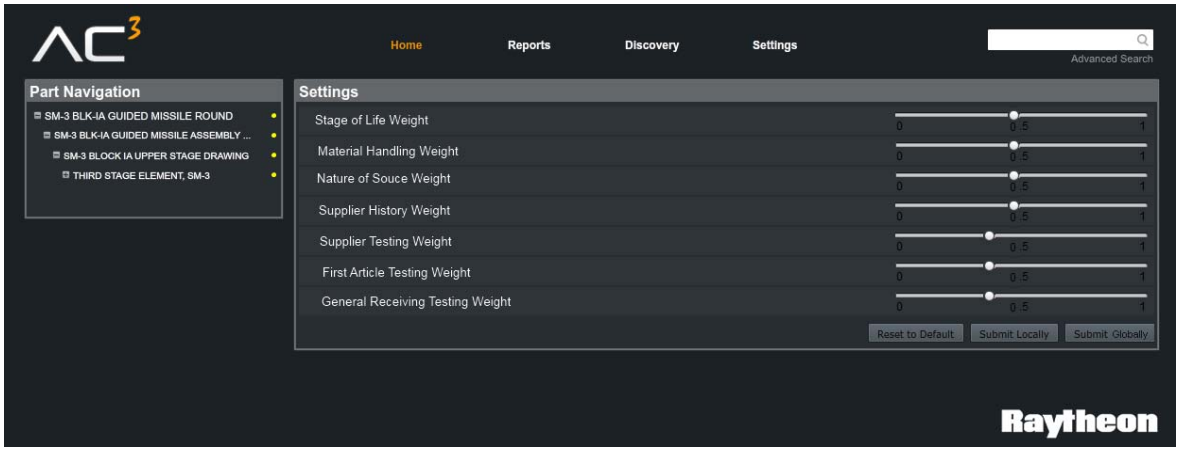
- Classification of the Supplier
  - Original Component Manufacturer
  - Franchised Distributor
  - Independent Broker
- Supplier History
  - Preferred Business Partner
  - Casual Business Partner
  - One Time Buy Source

Nature of Testing

- Supplier Testing
  - Credentialed and Monitored
  - Measure Driven and Monitored
  - Qualitative Visual Assessment
- First Article Testing
  - Prescriptive Testing By Article
  - Prescriptive Testing By Lot
  - General Testing By Lot
- General Receiving Testing
  - Prescriptive Testing By Article
  - Prescriptive Testing By Lot
  - General Testing By Lot

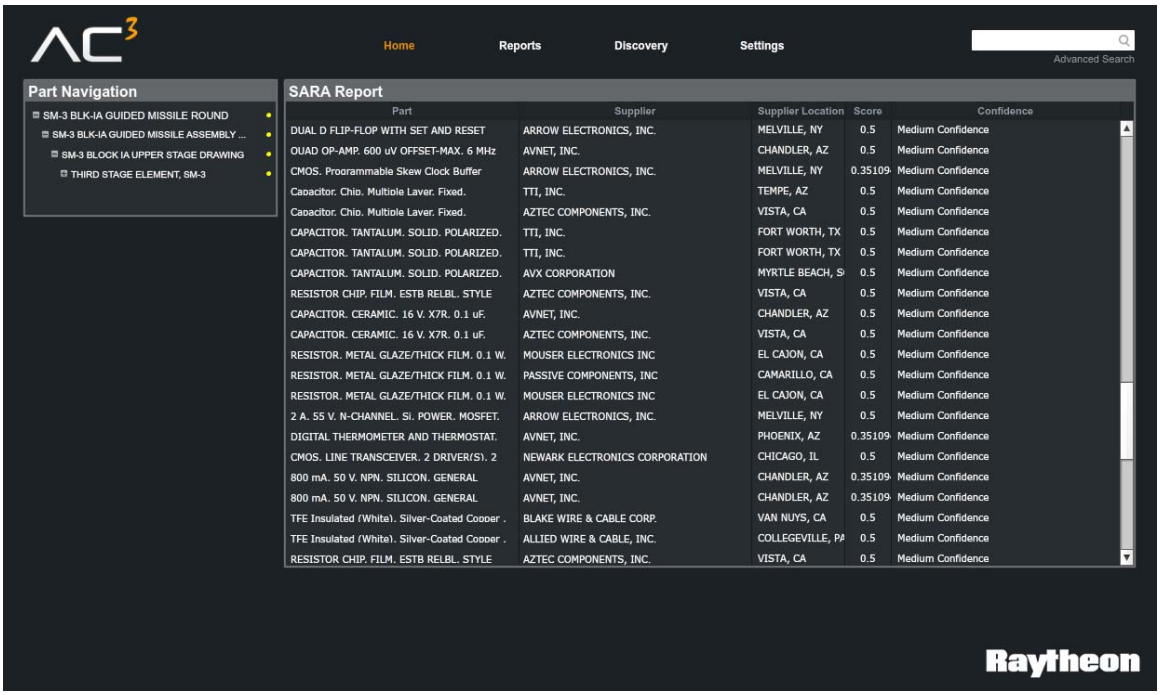
Within AC^3, each part and material that comprises a system is classified according to a program manager approved criticality assignment matrix that reflects all inputs to the criticality designation decision such as the MDA PMAP, RMS specific guidance, and acquisition contract specific guidance. Each criticality class maps to a program manager approved risk profile that sets an "alarm threshold" that is triggered when a part that violates one or more criticality class SARA input value thresholds enters the production process. A screen shot of the SARA administrative page is illustrated below. In the screen shot, the seven attribute values deemed as minimum acceptable for the specific criticality class are shown. The SARA algorithm is capable of using different administrator variable weighting schemes for each criticality class in order to tune alarm thresholds to meet user needs and set appropriate alarm thresholds.

Figure 2: AC^3 User Interface



The system allows the user group to continuously monitor the parts and materials being consumed in the production process as SARA continuously polls contributing data sources on a data specific refresh cycle. SARA supports a continuous risk topology assessment by the program manger helping prevent risk creep that takes place as incremental changes take place over time. With SARA, the program manager is notified of the impact of changes. When an input value changes, SARA runs an assessment and generates alerts as required.

Figure 3: AC^3 SARA Display



As an example of the utility of the proactive risk assessment approach, a part for which the program manager has specified a Franchised Distributor purchase requirement is sourced by a buyer from an

Independent Broker due to non-availability. The entry of the broker purchased parts into the production inventory is identified and the program manager is notified providing a SARA report detail. The program manager may assess the purchase and establish a condition that a prescriptive acceptance test be conducted on each article purchased. SARA records the guidance and updates the risk alarm profile for the specific part or material. Items failing to meet the updated risk guidance will generate alarms for further action by the program manager.

2.3 REACTIVE COUNTERFEIT RISK ASSESSMENT

Processing alerts is an inherently reactive process that is comprised of four major stages as illustrated below. Within the process, the critical measures of interest are elapsed time from alert to resolution and information accuracy. By quickly and accurately identifying the extent of the impact of an alert message quickly and accuracy can lead to significant savings in level of effort, hard costs, and downstream liability. The objective when a part or material alert is received is to identify if there is an impact, quantify the extent of the impact, and minimize the potential for the impact to increase during the resolution decision time frame.

Figure 4: Risk Assessment Process

Each of the four stages is described below pointing out the stage objective and stage specific challenges that delay progress.

2.3.1 ALERT

What is the nature of the alert? Knowing the subject of the alert, whether it's Failure Experience (counterfeit, suspect unapproved), Safe Alert, obsolescence, etc. and where it originates from Government-Industry Data Exchange Program (GIDEP), MDA, NASA, Raytheon internal, etc.

are important in determining the alert's priority. For example, the urgency associated with a counterfeit is in most cases higher than that associated with obsolescence.

2.3.2 INVESTIGATION

An investigation determines if and where vulnerabilities exist. Significant effort can be saved if the part/family in the alert is not found or referenced in the internal systems. Intelligent system searches help to determine if the part(s) are in the design or inventory and if so, the scope of the problem.

Where are they, what programs are affected and where did they come from (who supplied them)? (ID), or Brokers and display the information in an intuitive user interface.

2.3.3 ANALYSIS

An analysis of the information from the investigation is needed to determine the following for both part(s) and supplier(s):

- Part Number or Material Criticality
- History
- Alternate available

2.3.4 RESOLUTION

Ultimately, a plan is put into action to drive towards alert closure. Any human intelligence such as decisions, assumptions, etc. should be captured along with the systems package and archived for future reference.

AC^3 PROOF-OF-CONCEPT DESIGN AND IMPLEMENTATIONDESIGN OF THE OPERATIONAL TEST

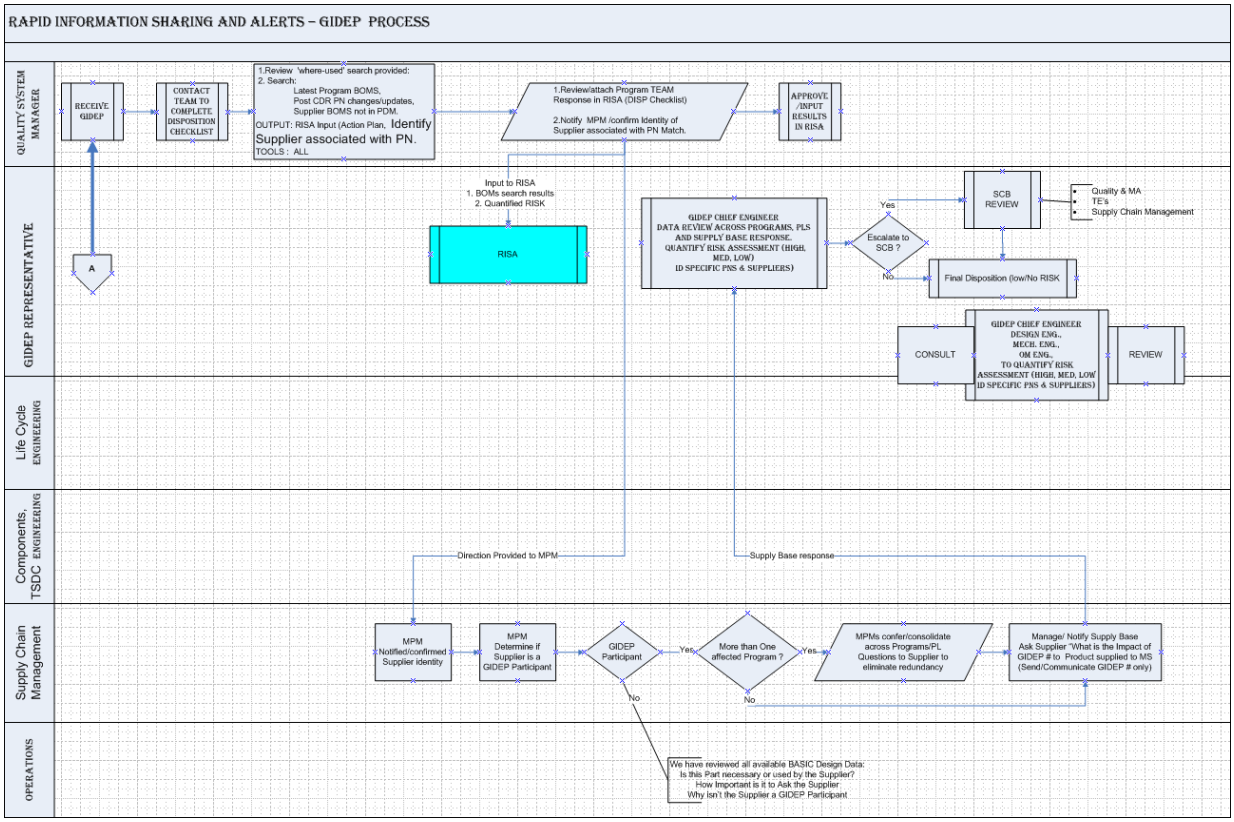
Operational testing was initially designed to use RMS's Rapid Information Sharing & Alerts (RISA) as a trigger mechanism signaling an alert search event within AC^3. The below step process was designed by the team to take place at the initial receipt of an alert to closing an alert:

1. An automated GIDEP alert received by RISA triggers a data transfer to AC^3
2. AC^3 receives RISA part number and/or supplier data and initiates enterprise level search
3. AC^3 correlates enterprise data and packages feed to RISA to pre-populate forms presented to subject matter experts (SME)
4. SME determines actionable information exists and "releases" the alert for program and / or organization level review and action
5. RISA sends AC^3 an "open" trigger and grants users access to data identifying part location by lot/date code and serial number
6. AC^3 and RISA track and record action taken by users (program and/or organization)
7. SME and program level managers determine satisfactory action is applied and "close" the alert in RISA (completed on a program-by-program, or organization basis for each Alert)
8. RISA sends AC^3 a "closed" trigger to archive the alert actions and mark the alert closed within both systems

Due to IT constraints, RISA trigger mechanisms and feeds were not developed or initiated. AC^3, instead, used manually entered part number and supplier data as the feed to trigger an enterprise level search and data correlation. The operational test continued without the RISA interface or open/close triggers. The SME and program managers conducted their research using AC^3 screens and reports to determine the level of impact a suspect part may have on RMS programs. This fix was sufficient to prove the concept; the automatic feed from RISA is a feasible enhancement.

Figure 5: Existing GIDEP Process Chart

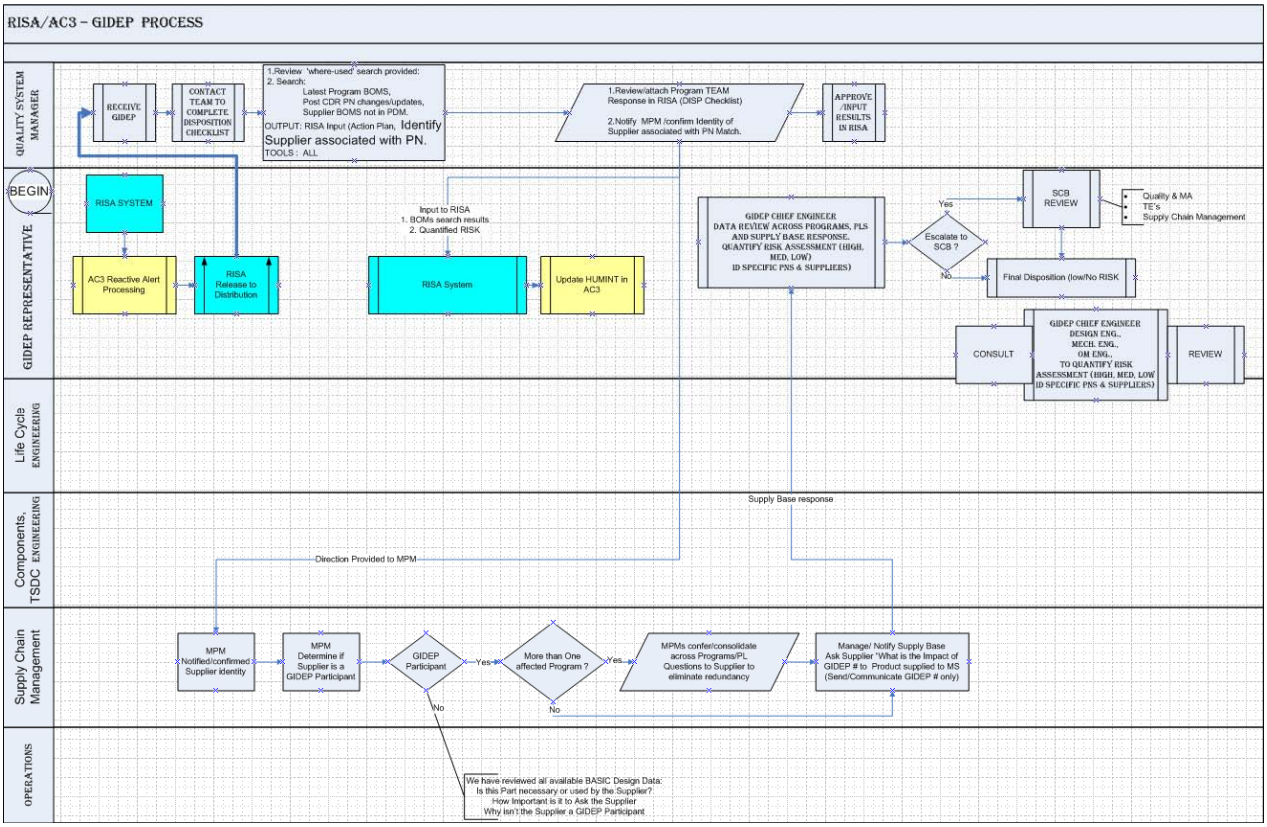
Process Mapping – Current Processes



The current GIDEP alerts process shown above is manually intensive with multiple opportunities for errors. The process is initiated by the Rapid Information Sharing & Alerts (RISA) system, the GIDEP Representative reviews the alert after which the task of investigating usage is completed by multiple organizations using multiple systems. Each organization returns the results of their findings which are consolidated into one report by the GIDEP Representative. This process involves coordinating and receiving research from five organizations taking approximately two calendar days (four hours of "touch" effort to complete.

2.2 PROCESS MAPPING – REVISED PROCESSES

Figure 6: Reused GIDEP Process



The AC^3 POC application fits in the GIDEP Alerts Process after the GIDEP Notification is received from RISA. AC^3 sends the compiled report to the RISA distribution. AC^3 takes over the research each organization is tasked with by searching the same systems automatically and consolidating the results into one report. 3.3 Comparison of the current and revised Processes

As part of the POC evaluation, process improvement metrics were established in key categories related to:

- Number of man-hours that were consumed to support an alert driven action
- Degree of human dependency for data review and integration
- Number of investigative path decisions that depend on human interpretation of digital data
- Time that the production process would continue in an "at-risk" state while the investigation into applicability was conducted

By taking over the research each organization is tasked with during a GIDEP Alert, the AC^3 POC was able to reduce the complexity of the GIDEP Alert process by automating the 6 decisions steps, 19 searches performed by 5 organizations, and data consolidation. The automations helped reduce the GIDEP Alert process from 4 hours effort over 2 calendar days to instantaneous. Opportunities for

errors due to data entry, fatigue and misinterpretation are also virtually eliminated by automating the search, evaluation and consolidation of the information into the report.

3 AC^3 DESIGN ASSESSMENT

One of the key project objectives was evaluation of the suitability of the design of the AC^3 software. To this end, the application was evaluated continuously through the design, deployment, and operational test phases to identify adjustments that should be made prior to full-scale deployment. The following is an analysis of the suitability of the software from several points of view:

- Alignment of the Use Cases with enterprise processes
- Feasibility of the Information Requirements
- Appropriateness of the System Architecture
- Utility of the System User Interface
- Relevance of Default Visualizations and Reports

3.1 ASSESSMENT OF THE USE CASES

Seven Use Cases were identified during the design phase of the project. Each was developed in response to MDA and prime contractor community stated needs. The following is a restatement of the Use Cases and an evaluation of the alignment with RMS enterprise processes.

3.1.1 USE CASE ONE: IDENTIFY THE PARTS AND MATERIALS ASSOCIATED WITH EACH ASSEMBLY WITHIN A SYSTEM

At the "core" of this POC which is to answer the question: "What happens when a counterfeit/suspect part enters the inventory?" Identifying where the suspect parts are located is the primary step to begin understanding the scope of an alert. The current RMS process involves six organizations to perform "where-used" type searches of various systems. AC^3 automates the search thereby simplifying the RMS process.

Alignment with RMS processes: HIGH

3.1.2 USE CASE TWO: IDENTIFY THE SUPPLY CHAIN LINEAGE ASSOCIATED WITH PARTS AND MATERIALS

AC^3 would provide the ability to identify the lineage or "pedigree" of parts/materials, which is highly desirable. Unfortunately, for many reasons, RMS and most of the industry is unable at this time to track the lineage of components/materials with any degree of confidence. However, it was universally agreed that the pedigree track capability would provide critical data currently lacking in many DoD weapons systems.

No comparative processes at RMS

Alignment with current RMS processes: LOW* but highly desirable

3.1.3 USE CASE THREE: CHARACTERIZE THE SOURCE OF THE PARTS AND MATERIALS BY SOURCE TYPE AS DEFINED BY THE PARTS MATERIAL AND PROCESSES MISSION ASSURANCE PLAN (PMAP)

As part of the GIDEP Alerts process, source characterization is used to quantity the risk associated with a particular supplier of interest. RMS currently identifies suppliers by "Supplier Type" in The Supplier Directory system, TSD.

Alignment with RMS processes: HIGH

3.1.4 USE CASE FOUR: ASSESS PAST PERFORMANCE OF SUPPLIERS OF INTEREST USING IN-PLACE SUPPLIER METRICS

RMS's Supplier Rating System (SRS) provides a consistent method of rating suppliers across the company. Use of the SRS tool to assist in the supplier selection process can reduce program risks and operating costs. The SARA algorithm in AC^3 takes the SRS inputs in the source category to provide a quantifiable risk indicator as described in 2.2 PROACTIVE RISK COUNTERFEIT ASSESSMENT.

Alignment with RMS processes: HIGH

3.1.5 USE CASE FIVE: IDENTIFY COUNTERFEIT RISK POTENTIAL CONSISTENT WITH THE RISK PARAMETERS IN THE PMAP

The risk potential provided by AC^3 used the parameters inherently associated with sourcing from OEM,OCM, FAD, Independent Distributors and Brokers etc. to classify the risk potential but does not directly use the actual physical receipt inspection results delineated in section 3.6.6 of the PMAP including: close examining of the Certificate of Conformance; Destructive Physical Analysis, Particle Impact Noise Detection; X-Ray Fluorescence or equivalent; Fourier Transform Infrared; ASTM; API; and SAE testing.

Alignment with RMS processes: MODERATE

3.1.6 USE CASE SIX: INVENTORY IN-PLACE RISK MITIGATION PRACTICES APPLICABLE TO A PART OR MATERIAL OF INTEREST

Identifying where the suspect parts from a lot purchase are located is the "core competence" and valued add of AC^3. The current RMS process involves six organizations to perform these types of searches.

Alignment with RMS processes: HIGH

3.1.7 USE CASE SEVEN: SEARCH THE CURRENT RMS SUPPLIER BASE AND THE GREATER INDUSTRIAL BASE FOR ALTERNATIVE SOURCES

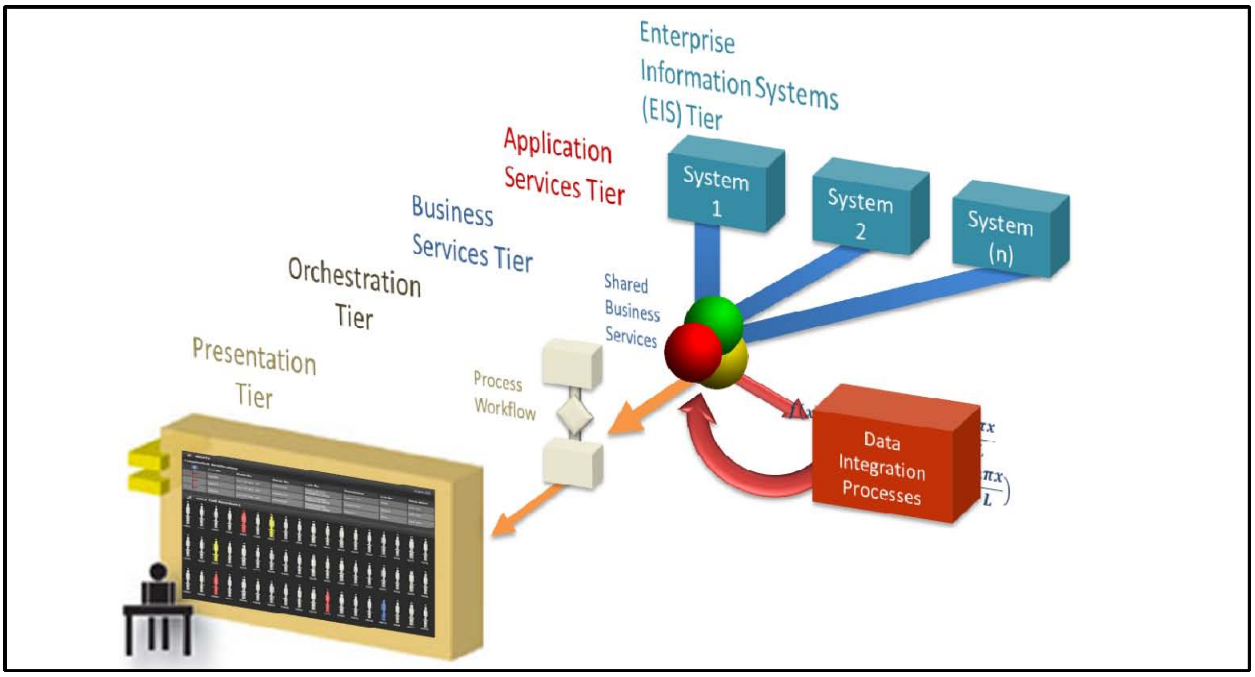
TSD currently provides search capabilities for currently active RMS suppliers. There is a gap when the needs are not met by the current supply base. AC^3 could provide alternative suppliers both

from the current TSD supplier database and external supplier databases by NAICS/SIC codes or separate web crawler searches of supplier websites.

Alignment with RMS processes: HIGH

3.2 ASSESSMENT OF THE INFORMATION REQUIREMENTS

Figure 7: AC^3 Information High Level Architecture



3.2.1 ENTERPRISE INFORMATION SYSTEMS (EIS) TIER

Table 4: RMS Data Systems Intergrated Into AC^3

CABS - Common As-Built System	**PRISM** - Process Re-inventing Integration Systems for Manufacturing
PDM - Product Data Management	**RISA** - Rapid Information Sharing & Alerts
CIMS- Component Information Management System- RMS parts information repository	

The AC^3 proof of concept final configuration is a web based application designed to capitalize on existing technologies for maximum input from subject matter experts and agility in development. It is based on ACC's modular service-oriented architecture (SOA) called Visual Supplier Assessment & Analysis Modules (VSAAM) and its RMS predecessor Mission Assurance supply chain Mapping Interface (MIAMI) application.

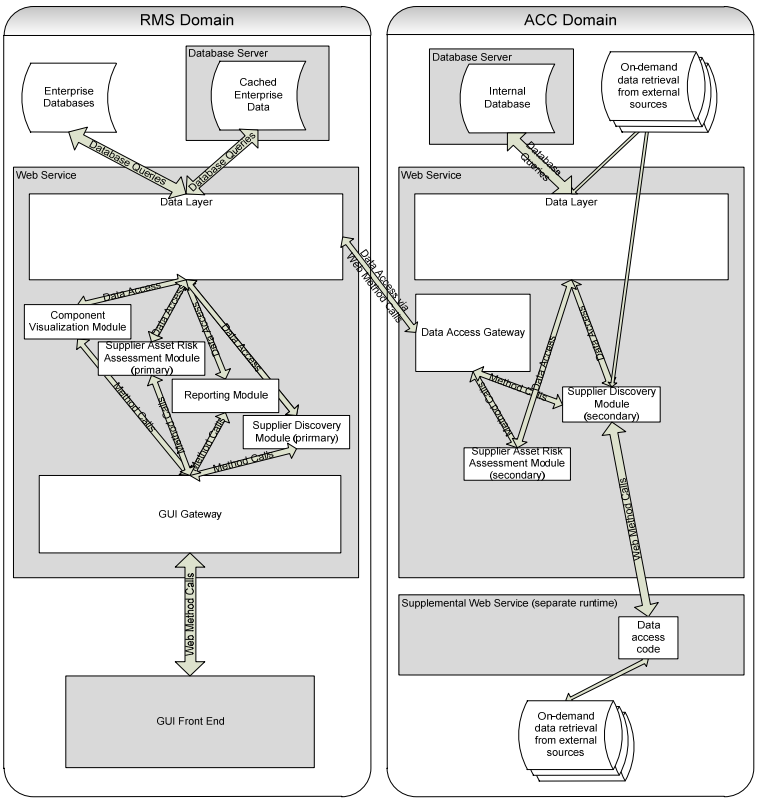
- **Component Visualization Module (CVM):** Provides a graphical view of components in an assembly or list allowing navigate up and down the assembly hierarchy from discrete component to assembly to system.
- **Supplier Asset Risk Assessment Module (SARA)**: A predictive assessment algorithm of counterfeit risk issues associated with a part and/or supplier.
- **Reporting Module (RM)**: User reports related to components, suppliers, and/or their related issues.
- **Supplier Discovery Module (SDM)**: Correlates RMS Supplier Directory in combination with ACC sources of supplier information, finds information about known suppliers, and identifies yet-unknown suppliers that may provide relevant services or parts.

The functionality of the application is limited to sufficiently demonstrate its capabilities in the range of parts covered in this proof-of-concept. Its requirements were defined in close cooperation with RMS-Tucson SCM and IT staff.

3.3 SYSTEM ARCHITECTURE

The AC^3 architecture is comprised of both internal RMS enterprise data sources and external web-services feeds correlated to provide users with a single view of potentially affected parts, their locations, and suppliers who may have interweaved the parts into the system.

Figure 8: AC^3 POC High Level Architecture – Physical View



AC^3 utilizes Microsoft SQL Server as the backend data repository for the POC which includes RMS enterprise data from systems listed in the table below. Due to time constraints and limited IT resource availability, functional experts were used to generate reports from each enterprise system as a feed to populate the dataset used for the POC. Each feed was imported using generated templates and data mapping to tie data elements from the lowest level component up to the highest level system.

Business logic tied individual data sources into cohesive export functions using Microsoft C#, Java, and JavaScript's as the middle layer of the application. The front end was designed using Adobe Flash for execution of function and user feedback mechanisms.

Table 5: AC3 Data Feeds

Source ID	Source Name	Relevant Data	Integration Strategy
Andover	Andover CCA BOMs	Bills of material for circuit card assemblies from Andover; include lot numbers and date codes for components	Data extracted and stored in an AC^3- database
CABS	Configuration As-Built System	Matches part serial numbers to tail numbers *for "accountable" items only*; can answer "where used" queries.	Data extracted and stored in an AC^3- database
PDM	Product Data Management / SHERPA	Bills of Material (BOMs) and part drawings in PDF format, part numbers (if source-controlled) or spec numbers in an assembly, next higher assembly.	Data extracted and stored in an AC^3- database
PRISM	Process Re-invention Integrating Systems for Manufacturing	Primary information storage for RMS business operations; contains Purchase Orders and many other pieces of data	Data extracted and stored in an AC^3- database
RISA	Rapid Information Sharing & Alerts	RMS alert system; alerts internally-generated and pulled from sources such as GIDEP	Past RISA alerts were studied to determine the quantity and quality in a typical event. Test events were generated in a style consistent with those findings. Generating test events is necessary because it is unlikely actual alerts will be generated for the small subset of parts covered in the AC^3 Proof-of-Concept during the trial period.

TSD	The Supplier Directory	Supplier information: name, ids, contact information, high-level ratings, capabilities, certifications, classifications	Data extracted and stored in an AC^3- database

3.3.1 SERVER

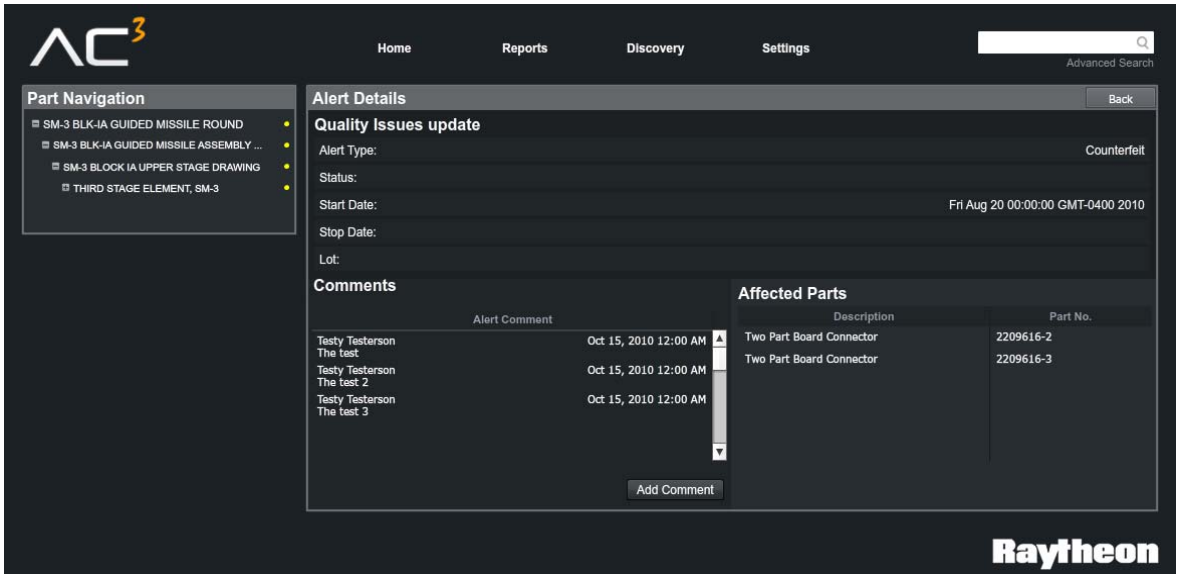
Due to the fact that AC^3 is a Proof of Concept (POC), RMS IT policy restricted the AC^3 software to a Virtual Machine operating with the following configuration:

Table 6: Server Characteristics

Xeon CPU 3.33 GHz	IIS V7.5
40 GB Disk	MS-SQL Server 2008 R2
4 GB RAM	MS NET Framework 4
MS Windows Server 2008 R2 Standard	

3.4 ASSESSMENT OF THE USER INTERFACE

Figure 9: AC3 User Interface



AC^3 reacts to alerts of counterfeit parts reported by GIDEP and then identifies the location of the parts within RMS programs, and suppliers who may have delivered a counterfeit part to RMS. Correlated data between the GIDEP alert and RMS enterprise systems is displayed using drill-down to access more detailed information about the alert.

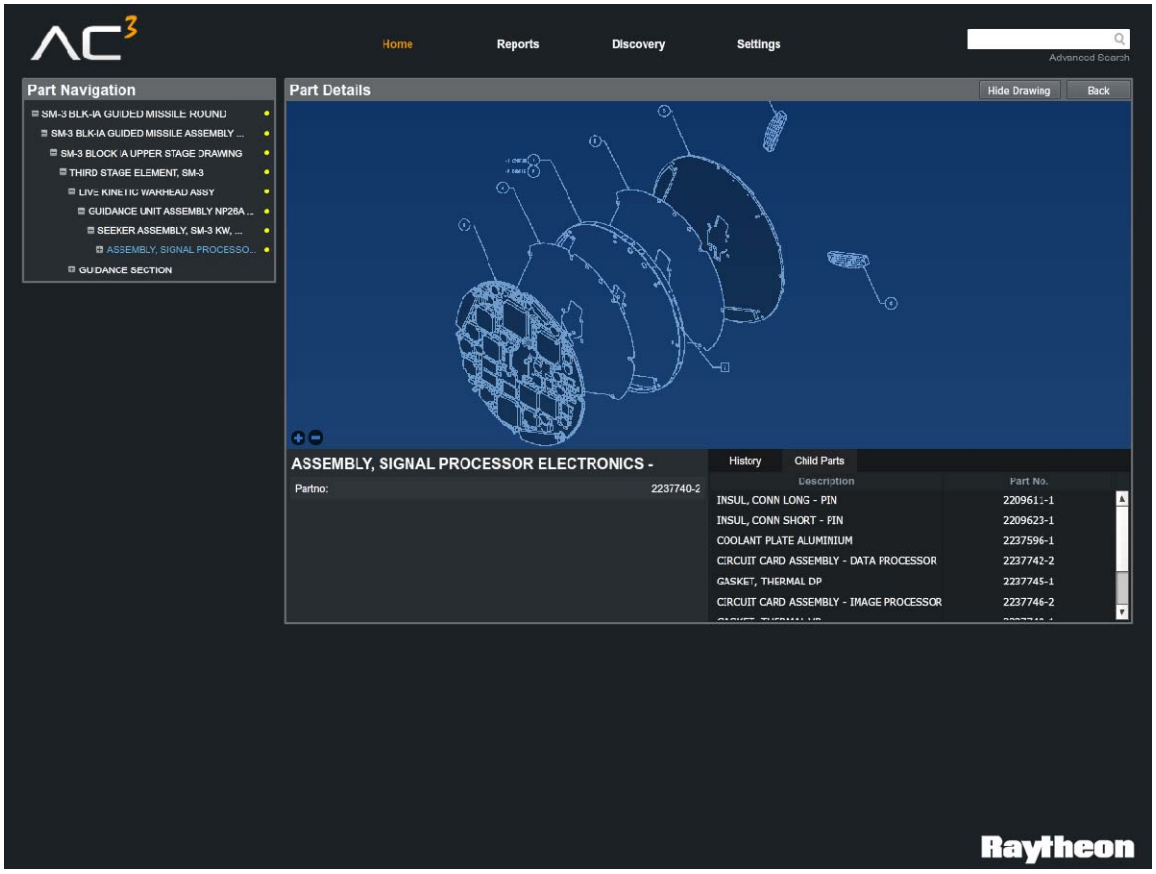
The user interface was designed to provide an at-a-glance visual representation of all open and closed GIDEP alerts. Open and closed alerts are displayed in descending date order with the newest open alerts highlighted at the top of the list followed by closed alerts retained for historical reference.

Historical alerts also capture human intelligence identifying all the steps taken to research and resolve past alerts. Users navigate the interface by mouse-clicking on top level menu options, left pane parts tree navigation, or right pane recent alerts list navigation. Top level menu options provide access to reports, the Supplier Discovery module, and user settings.

3.5 ASSESSMENT OF THE VISUALIZATIONS AND REPORTS

Visualization and reporting are used throughout the application to help identify suspect counterfeit parts location and status. Illustrations from the PDM system were captured and converted to scalable vector graphics to help users visualize where suspect parts fit within the SM3 missile. Code added to the illustrations highlights the suspect parts to focus attention both in a hierarchal tree structure view and an illustrated parts breakout view. Navigation is simplified by allowing users to click on "hotspots" for quick access to multiple levels of the SM3 system structure.

Figure 10: AC3 Subsystem Component Parts Display



3.5.1 SECURITY

AC^3 is located behind the RMS firewall and relies entirely on the IT engineers for security measures. The need for additional internal program security was not necessary because of the adequate features inherently associated with a large organization's policies and procedures that govern access to their enterprise servers and data systems.

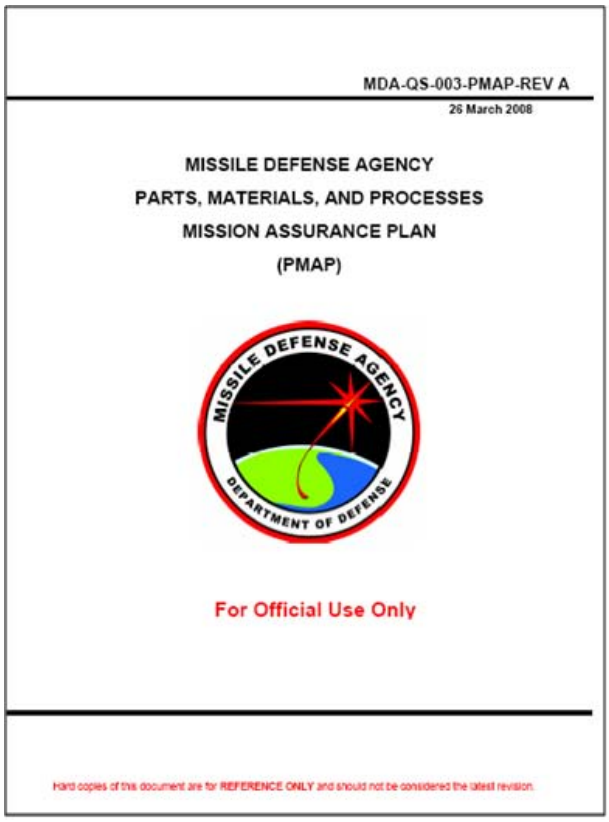
4 PROOF-OF-CONCEPT (POC) FINDINGS

As part of the POC, the AC^3 software application was measured against a set of performance objectives and measures. The performance objectives were developed by examining the MDA data reporting requirements for prime contractors with respect to anti-counterfeiting efforts. The source documents for the objectives were the MDA PMAP and a recently developed MDA Audit Questionnaire. Performance objectives provide a policy compliance assessment of the utility of the AC^3 software application. These performance objectives were supplemented by process effectiveness performance measures which were developed by the joint TDSC – RMS team. In total, the performance measures provide insight into the ability of the AC^3 software application to perform its data assessment and to generate decision quality information.

4.1 PERFORMANCE OBJECTIVES (POLICY COMPLIANCE)

The MDA Parts Materials and Processes Mission Assurance Plan (PMAP) (March 2008) provides compliance guidance that applies to new start MDA systems and to major block upgrades to current and legacy systems. The PMAP provides guidance on part and material practices in terms of sourcing, tracing, and testing according to MDA defined criticality classes. The MDA Anti-Counterfeiting Practices Audit (November 2010) provides the measures of evaluation and accountability for use in MDA review of anti-counterfeiting practices.

Figure 11: MDA PMAP Audit Questions


MDA-QS-003-PMAP-REV A

26 March 2008

MISSILE DEFENSE AGENCY

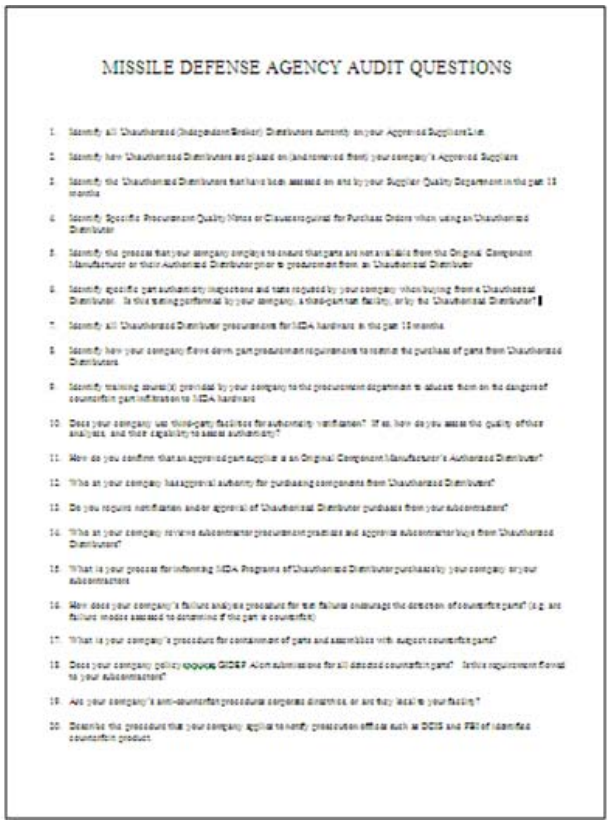
PARTS, MATERIALS, AND PROCESSES

MISSION ASSURANCE PLAN

(PMAP)

For Official Use Only

Hard copies of this document are for REFERENCE ONLY and should not be considered the latest revision.


MISSILE DEFENSE AGENCY AUDIT QUESTIONS

1. Identify all 'Unauthorized (Independent Broker)' Distributors currently on your Approved Suppliers List.
2. Identify how 'Unauthorized Distributors are placed on (and removed from) your company's Approved Suppliers
3. Identify the 'Unauthorized Distributors that have been assessed on site by your Supplier Quality Department in the past 18 months
4. Identify Specific Procurement Quality Notes or Clauses required for Purchase Orders when using an Unauthorized Distributor
5. Identify the process that your company employs to ensure that parts are not available from the Original Component Manufacturer or their Authorized Distributor prior to procurement from an 'Unauthorized Distributor
6. Identify specific part authenticity inspections and tests required by your company when buying from a 'Unauthorized Distributor. Is this testing performed by your company, a third-party lab facility, or by the 'Unauthorized Distributor?
7. Identify all 'Unauthorized Distributor procurements for MDA hardware in the past 18 months
8. Identify how your company flows down part procurement requirements to restrict the purchase of parts from 'Unauthorized Distributors
9. Identify training source(s) provided by your company to the procurement department to educate them on the dangers of counterfeit part infiltration to MDA hardware
10. Does your company use third-party facilities for authenticity verification? If so, how do you assess the quality of their analyses, and their capability to assess authenticity?
11. How do you confirm that an approved part supplier is an Original Component Manufacturer's Authorized Distributor?
12. Who at your company has approval authority for purchasing components from 'Unauthorized Distributors'
13. Do you require notification and/or approval of 'Unauthorized Distributor purchases from your subcontractors?
14. Who at your company reviews subcontractor procurement practices and approves subcontractor buys from 'Unauthorized Distributors'
15. What is your process for informing MDA Programs of 'Unauthorized Distributor purchases by your company or your subcontractors
16. How does your company's failure analysis procedure for test failures encourage the detection of counterfeit parts? (e.g. are failure modes assessed to determine if the part is counterfeit)
17. What is your company's procedure for containment of parts and assemblies with suspect counterfeit parts?
18. Does your company policy require GIDEP Alert submissions for all detected counterfeit parts? Is this requirement flowed to your subcontractors?
19. Are your company's anti-counterfeit procedural changes dynamic, or are they static in your facility?
20. Describe the procedure that your company applies to notify prosecution offices such as DCIS and FBI of identified counterfeit product.

The two documents were reviewed to determine the applicability of AC^3 in supporting prime contractors in their efforts to comply. Key performance objectives extracts are presented below along with the fulfillment assessment.

4.1.1 PMAP AREA ONE: SUPPLIER INFORMATION BY PART/MATERIAL

Requirement: The PMAP requires that supplier records indicate the source of supply and classification of the supplier as an OCM, a FAD, or an IB. For parts and materials purchased from an IB, the PMAP requires, based on criticality class, that the supplier be approved by MDA.

4.1.2 PMAP AREA TWO: LOT/DATE CODE OR SERIAL NUMBER TRACKING BY PART/MATERIAL

Requirement: The PMAP requires that all parts and materials be tracked at either the lot/date code level or the serial number level depending on part/material criticality class.

4.1.3 PMAP AREA THREE: QUALIFICATION AND TESTING DATA TRACKING BY LOT/DATE CODE OR SERIAL NUMBER

Requirement: The PMAP requires general and/or prescriptive testing practice and objective specification compliance for each defined part/material class.

Finding: AC^3 supports the continuous maintenance of records that require integration of data from disparate parts of the enterprise. Supplier data, purchase records, testing records, and configuration records are integrated to provide a round by round pedigree that supports instantaneous searches to identify the content, the sources, and qualification compliance. AC^3 supports a markedly advanced capability from the current environment in which record individual searches and human integration efforts would be required to respond to a query. AC^3 provides a cost effective means to call on the available data to produce the highest degree of clarity possible given the contract flow-down requirements for part and material traceability required by the PMAP.

4.1.4 MDA AUDIT AREA ONE: ACCOUNTABILITY OF SUPPLIERS THAT ARE INDEPENDENT BROKERS

Requirement: Identify all Unauthorized (Independent/Broker) Distributors currently on your Approved Suppliers List. Identify all Unauthorized Distributor procurements for MDA hardware in the past 18 months.

4.1.5 MDA AUDIT AREA TWO: RECORD OF CONDITIONS PLACED ON INDEPENDENT BROKER BUYS

Requirement: Identify Specific Procurement Quality Notes or Clauses required for Purchase Orders when using an Unauthorized Distributor. Identify specific part authenticity inspections and tests required by your company when buying from an Unauthorized Distributor and indicate if this testing is performed by your company, by a third-part test facility, or by the Unauthorized Distributor.

4.1.6 MDA AUDIT AREA THREE: RECORD OF INDEPENDENT BROKER APPROVALS

Requirement: Identify who at your company has approval authority for purchasing components from Unauthorized Distributors. Identify how your company flows down part procurement requirements to restrict the purchase of parts from Unauthorized Distributors.

Finding: AC^3 supports each of the three MDA Anti-Counterfeiting Audit areas identified above. AC^3 currently has the ability to poll the classicization (OCM, FAD, IB) for all suppliers within a particular program. In addition, AC^3 supports generation of a cross reference list identifying all other parts provided by an Independent Broker and identifying the programs supported by procurements form the Independent Broker of interest. The SARA algorithm allows program managers to specify practices for each part and material based on MDA and/or internal requirements. For parts that are granted a conditional Independent Broker procurement authorization, AC^3 provides record access to identify the quality notes and inspection practices required as part of program manager specified risk mitigation strategies. AC^3 allows authorized individuals to make changes to the risk reporting thresholds within the system and supports retention of human intelligence in the form of a record of decisions and conditions maintained in a blog-style format.

4.2 PERFORMANCE MEASURES (PROCESS EFFECTIVENESS)

Through the course of the project, the joint TDSC-RMS team collected and evaluated process effectiveness measures. These were identified in discussions with personnel at various levels across multiple enterprise functions including program management, data management, supply chain management, quality assurance management, obsolescence management, and GIDEP management. From these discussions several performance metrics addressing process effectiveness were identified and evaluated on a "go or no-go" basis as identified in the figure below.

Table 7: Evaluation Metrics

	METRIC	CRITERIA FOR SUCCESS	Assessment
1	Demonstrate a comprehensive, integrated system that provides rapid, highly detailed visibility into the extended supply chain at the discrete part level.	Go-No Go as decided by RMS	
2	Successful implementation of the AC^3 system in a pilot environment on a critical sub-system of the Standard Missile Three (SM-3) weapons system.	Go-No Go as decided by RMS	
2a	# & % of electronic component parts that can be automatically traced to a source (OCM, OEM, FAD, ID, or broker)	Go-No Go as decided by RMS	
2b	# & % of RMS component suppliers with unauthorized parts procurement.	Go-No Go as decided by RMS	
2c	For a given critical system circuit card assembly (CCA), determine the risk assessment and individual CCA risk ranking among all CCA in a particular SM-3 system.	Go-No Go as decided by RMS	
2d	Identify at least one alternative source for every critical SM-3 CCA.	Go-No Go as decided by RMS	

Finding: AC^3 provided a first-ever end-to-end automated alert process management framework. The application was evaluated by walking through the manual process step by step and comparing the information generation capabilities of the application with those that have been developed and employed over time. The application provided a flexible assessment environment allowing examination of the problem within the proof-of-concept scope. Data was accessible via several query paths that the GIDEP team has developed allowing an assembly logic drill-down, a part number search, a supplier search, and a supplier-part-program cross-reference search. Supplier classification was readily displayed reflecting the details contained in the supplier directory. Test case alerts were generated to trigger warning messages allowing free-form investigation. The SARA algorithm was demonstrated to support risk ranking based on part and material criticality class as defined by government, corporate, and program manager guidance. For Measure 2d, due to funding limitations, the function was demonstrated at the bread-board level based on comparison of North American Industrialization Classification System (NAICS) codes. Other technologies have been demonstrated such as webcrawlers to investigate individual websites and search for certain lexicon terms. However, the current RMS TSD supplier directory data base being investigated already has the supplier capabilities identified.

5 SUMMARY AND CONCLUSIONS

AC^3 was **successfully** deployed in a proof-of-concept format using real world data and electronics intensive guidance sub-assemblies within SM-3. The proof-of concept application was evaluated using key measures identified by the joint TDSC – RMS project team including: the number of man-hours that were consumed to support an alert driven investigative action, the degree of human dependency for data review and integration, the number of investigative path decisions requiring human

interpretation of digital data, and the time that the production process would continue in an "at-risk" state while the investigation was conducted.

Through implementation of AC^3 the complexity of the RMS GIDEP Alert process was reduced by automating 19 independent data searches performed by 5 organizations supporting 6 human-in-the-loop decision points. Automation reduced the level of effort, the dependency on human data interpretation, and the elapsed investigate time. The results are summarized below.

Table 8: GIDEP Process Comparison

	Man-hours	Human Information Integration Dependency	Human Investigative Path Decisions	Investigative Time
W/O AC^3	20 hours	Very High	6	48 hours
W/ AC^3	< 30 minutes	Very Low	1	< 30 minutes

These improvements are significant as the number of alerts is expected to increase from 4-5 per month to 40-50 per week due to evolution of GIDEP policies designed to aggressively address the counterfeit issue. The team received a list of suspect counterfeit parts from Tom Sharpe of SMT Corporation. 147 suspect parts were screened using the AC^3 system. There were no potentially counterfeit parts on the list installed in the SM3 weapons system. The time required to run the check was minimal. The part number, date and lot code information were available in a spreadsheet and the information was run through the system in a few minutes time. Manually checking for installation would have taken significantly longer, perhaps days.

AC^3 operates as a Service Oriented Architecture within the enterprise Information Technology environment. AC^3 is deployed behind the corporate firewall calling on data generated and housed in enterprise0wide and functional area specific databases via a standing report protocol and a virtual data warehouse. Minimal data requirements include supplier records, purchasing records, testing records, design data, and configuration management records. AC^3 is readily extensible into a full-scale deployment offering a cost effective means of implementing MDA and DoD required practices to reduce the potential for counterfeit incursion.

6 NOTES ON EXPANSION AND DEPLOYMENT

The AC^3 proof-of-concept scope was limited to sub-assemblies and components for which the required pedigree data-tracking of individual components by lot number and date code- was readily available for the Raytheon Andover provided parts, but not other parts. The scope limitation was required because MDA production contracts implemented prior to the PMAP do not require collection and recording of lot number and date codes information. Full utilization of the visibility advances of AC^3 or any similar system is dependent on collection of such component tracking data. The MDA Parts Materials and Processes Mission Assurance Plan requires weapons systems and major block upgrades implemented after the effective date of March 2008 to be fully PMAP compliant; "All materials shall be traceable to manufacturer and production lot or date code. Documentation shall be in place to provide bi-directional traceability of materials from receipt to the highest assembly level".

Upgrading legacy systems prior to 2008 to track this information is an extensive and expensive task for the prime contractors and the entire supply chain who have not implemented the capability thus far. There is reluctance to incur any costs associated with implementing these changes without a corresponding value proposition or cost savings incentive, especially in austere budget times. It is hoped that implementation at RMS will provide that incentive

The AC^3 proactive counterfeit risk reduction function embodied in the SARA was designed to support the development of data enrichment strategies providing insight into the risk location by component and risk classification by criticality supporting prioritization of effort. For each of the priority components, SARA supports identification of the data elements that would have the highest beneficial impact supporting definition of effort and identification of the cost associated with incremental data gap closure.

Moving forward, programs which come under the authority of PMAP will be required to capture the lot number and date code to fully realize AC^3 type of capabilities. Legacy and future programs that do not fall under the authority of PMAP will have to make a business decision which balances the risk versus the cost of obtaining the PMAP type information.

The AC^3 team has had several meetings with RMS Six Sigma personnel, speaking with Kathleen Reilly, Frank Bernard, Warren Hatcher and others to deploy the system. This internal Six Sigma process was used previously when the Supply Chain Technologies for Affordable Missile Programs (STAMP) demonstrated significant savings and quality potential associated with using an automated technical data package creation and delivery system which is in use at RMS today. It is hoped that RMS leaders will note the value of integrating the AC^3 system into their production processes and pay the modest costs associated with implementation.